THE OHIO STATE BOARD OF PHARMACY

Policy for Maintaining a Log of Access to Confidential Personal Information

1.0 Purpose

The Ohio State Board of Pharmacy (the Board) remains committed to ensure the privacy and security of the information of Ohio's citizens that is stored with the agency. This policy implements principles, procedures and practices that safeguard Ohio's Citizens' personal information within the Board's control.

2.0 Scope

This policy applies to all data maintained by the Board containing confidential personal information and employees requiring access to such information. Ohio Revised Code Section 1347.15 requires the Board, and all other state agencies, to treat certain personal information confidential, and to limit employee access to such personal information. Ohio Administrative Code Section 4729-1-11(E) requires the Board to issue a policy specifying the procedures for the maintenance of a log of access to confidential personal information. This Policy is promulgated pursuant to the above-stated rules and laws.

3.0 Definitions

The definition of terms used within this policy can be found in Ohio Administrative Code Section 4729-1-07 reprinted in Section 9.0 herein.

"Confidential Personal Information Log" means the file of Access Incident Reports maintained by the data privacy point of contact.

"Access Incident Report" means the paper form filled out by an employee or his/her supervisor recording any incident of invalid access to Confidential Personal Information, attached.

4.0 Compliance

All employees of the Board shall read and adhere to the mandates of Ohio Revised Code Section 1347.15 and Ohio Administrative Code Sections 4729-1-07 through 4729-1-11. Any violation of the rules and laws regarding the access of confidential personal information maintained in any format by the Board shall be immediately reported pursuant to the Reporting Chain identified in Section 5.1 of this policy. An Access Incident Report shall be completed by the employee and his/her supervisor. A copy of

the Access Incident Report shall be provided to the data privacy point of contact identified in Section 5.2 of this policy.

Valid access of confidential personal information maintained by the Board not otherwise logged pursuant to Ohio Revised Code Section 1347.15(B)(4)(a) must also be reported on an Access Incident Report. Such Reports shall be submitted to the appropriate executive supervisory staff member identified in Section 5.1 of this policy.

The data privacy point of contact identified in Section 5.2 of this policy shall maintain a file of all Access Incident Reports. Such reports shall be kept for a period of two years from the date of completion. The data privacy point of contact shall verify collection of all Access Incident Reports as needed with all executive supervisory staff members identified in Section 5.1 of this policy. The data privacy point of contact shall work with the Chief Privacy Officer designated by the State of Ohio and referenced in Section 5.3 of this policy to ensure compliance with all applicable rules and laws concerning the maintenance of and access to confidential personal information.

5.0 Reporting Chain Procedures

5.1 Reporting Chain

Any and all violations of Ohio Administrative Code Section 4729-1-09 shall be immediately reported pursuant to the following chain of command. Such violations shall be documented on an Access Incident Report. All employees shall report their own violations as well as any suspected or observed violations of other employees. Failure to report violations will result in disciplinary action.

The **Legislative Affairs Administrator** shall collect reports from the following employees under his/her supervision:

- Fiscal Officers
- Account Clerks
- Office Assistants

The **PMP Administrator** shall collect reports from the following employees under his/her supervision:

- Database Administrators
- Data Analysts
- Administrative Assistants

The **Assistant Executive Director** shall collect reports from the following employees under his/her supervision:

- Compliance Supervisors
- Compliance Specialists
- Field Supervisors
- Compliance Agents
- Administrative Assistants

The **Legal Affairs Administrator** shall collect reports from the following employees under his/her supervision:

- Executive Secretaries
- Administrative Assistants

The **Licensing Administrator** shall collect reports from the following employees under his/her supervision:

- Information Systems Administrators
- Programmers/Analysts
- Certification/Licensing Examiners
- Administrative Assistants

Any violations of OAC 4729-1-09 committed by the Executive Director, the Executive Director's Executive Secretary, the above-identified executive staff or the assigned Assistant Attorney General shall be reported directly to the Data Privacy Point of Contact.

Any employee not specifically named in the reporting chain outlined above shall report violations through their chain of command identified at hire.

5.2 Data Privacy Point of Contact

The Data Privacy Point of Contact shall be the Licensing Administrator.

5.3 Chief Privacy Officer

The Chief Privacy Officer is designated by the State of Ohio Privacy and Security Information Center, a Department of Administrative Services sub-section.

6.0 Penalties for Non-Compliance

Any employee that violates the mandates of this Policy, Ohio Revised Code Section 1347.15, or Ohio Administrative Code Sections 4729-1-07 through 4729-1-11 is subject to the following discipline:

Pursuant to Ohio Revised Code Section 124.341:

(1)Removing or suspending the employee from employment;

(2) Withholding from the employee salary increases or employee benefits to which the employee is otherwise entitled;

(3) Transferring or reassigning the employee;

(4) Denying the employee promotion that otherwise would have been received;

(5) Reducing the employee in pay or position.

Pursuant to Ohio Revised Code Section 1347.99:

> Whoever violates division (H)(1) or (2) of section 1347.15 of the Revised Code is guilty of a misdemeanor of the first degree.

Pursuant to Ohio Revised Code Section 1347.15(G):

> Any employee that violates the mandates of this Policy, Ohio Revised Code Section 1347.15, or Ohio Administrative Code Sections 4729-1-07 through 4729-1-11 is subject to a civil action in the court of claims for money damages.

Pursuant to Ohio Revised Code Section 1347.15(H)(3):

> No state agency shall employ a person who has been convicted of or pleaded guilty to knowingly accessing or disclosing confidential information when such access or disclosure is prohibited.

8.0 Ohio Revised Code Section 1347.15

1347.15 Access rules for confidential personal information.

(A) As used in this section:

(1) "Confidential personal information" means personal information that is not a public record for purposes of section 149.43 of the Revised Code.

(2) "State agency" does not include the courts or any judicial agency, any state-assisted institution of higher education, or any local agency.

(B) Each state agency shall adopt rules under Chapter 119. of the Revised Code regulating access to the confidential personal information the agency keeps, whether electronically or on paper. The rules shall include all the following:

(1) Criteria for determining which employees of the state agency may access, and which supervisory employees of the state agency may authorize those employees to access, confidential personal information;

(2) A list of the valid reasons, directly related to the state agency's exercise of its powers or duties, for which only employees of the state agency may access confidential personal information;

(3) References to the applicable federal or state statutes or administrative rules that make the confidential personal information confidential;

(4) A procedure that requires the state agency to do all of the following:

(a) Provide that any upgrades to an existing computer system, or the acquisition of any new computer system, that stores, manages, or contains confidential personal information include a mechanism for recording specific access by employees of the state agency to confidential personal information;

(b) Until an upgrade or new acquisition of the type described in division (B)(4)(a) of this section occurs, except as otherwise provided in division (C)(1) of this section, keep a log that records specific access by employees of the state agency to confidential personal information;

(5) A procedure that requires the state agency to comply with a written request from an individual for a list of confidential personal information about the individual that the state agency keeps, unless the confidential personal information relates to an investigation about the individual based upon specific statutory authority by the state agency;

(6) A procedure that requires the state agency to notify each person whose confidential personal information has been accessed for an invalid reason by employees of the state agency of that specific access;

(7) A requirement that the director of the state agency designate an employee of the state agency to serve as the data privacy point of contact within the state agency to work with the chief privacy officer within the office of information technology to ensure that confidential personal information is properly protected and that the state agency complies with this section and rules adopted thereunder;

(8) A requirement that the data privacy point of contact for the state agency complete a privacy impact assessment form; and

(9) A requirement that a password or other authentication measure be used to access confidential personal information that is kept electronically.

(C)(1) A procedure adopted pursuant to division (B)(4) of this section shall not require a state agency to record in the log it keeps under division (B)(4)(b) of this section any specific access by any employee of the agency to confidential personal information in any of the following circumstances:

(a) The access occurs as a result of research performed for official agency purposes, routine office procedures, or incidental contact with the information, unless the conduct resulting in the access is specifically directed toward a specifically named individual or a group of specifically named individuals.

(b) The access is to confidential personal information about an individual, and the access occurs as a result of a request by that individual for confidential personal information about that individual.

(2) Each state agency shall establish a training program for all employees of the state agency described in division (B)(1) of this section so that these employees are made aware of all applicable statutes, rules, and policies governing their access to confidential personal information.

The office of information technology shall develop the privacy impact assessment form and post the form on its internet web site by the first day of December each year. The form shall assist each state agency in complying with the rules it adopted under this section, in assessing the risks and effects of collecting, maintaining, and disseminating confidential personal information, and in adopting privacy protection processes designed to mitigate potential risks to privacy.

(D) Each state agency shall distribute the policies included in the rules adopted under division (B) of this section to each employee of the agency described in division (B)(1) of this section and shall require that the employee acknowledge receipt of the copy of the policies. The state agency shall create a poster that

describes these policies and post it in a conspicuous place in the main office of the state agency and in all locations where the state agency has branch offices. The state agency shall post the policies on the internet web site of the agency if it maintains such an internet web site. A state agency that has established a manual or handbook of its general policies and procedures shall include these policies in the manual or handbook.

(E) No collective bargaining agreement entered into under Chapter 4117. of the Revised Code on or after the effective date of this section shall prohibit disciplinary action against or termination of an employee of a state agency who is found to have accessed, disclosed, or used personal confidential information in violation of a rule adopted under division (B) of this section or as otherwise prohibited by law.

(F) The auditor of state shall obtain evidence that state agencies adopted the required procedures and policies in a rule under division (B) of this section, shall obtain evidence supporting whether the state agency is complying with those policies and procedures, and may include citations or recommendations relating to this section in any audit report issued under section 117.11 of the Revised Code.

(G) A person who is harmed by a violation of a rule of a state agency described in division (B) of this section may bring an action in the court of claims, as described in division (F) of section 2743.02 of the Revised Code, against any person who directly and proximately caused the harm.

(H)(1) No person shall knowingly access confidential personal information in violation of a rule of a state agency described in division (B) of this section.

(2) No person shall knowingly use or disclose confidential personal information in a manner prohibited by law.

(3) No state agency shall employ a person who has been convicted of or pleaded guilty to a violation of division (H)(1) or (2) of this section.

(4) A violation of division (H)(1) or (2) of this section is a violation of a state statute for purposes of division (A) of section 124.341 of the Revised Code.

Effective Date: 2008 HB648 04-07-2009

9.0 Ohio Administrative Code Sections 4729-1-07 through 4729-1-11

4729-1-07 DEFINITIONS; PERSONAL INFORMATION SYSTEMS

For the purposes of administrative rules promulgated in accordance with section 1347.15 of the Revised Code, the following definitions apply:

(A) "Access" as a noun means an opportunity to copy, view, or otherwise perceive whereas "access" as a verb means to copy, view, or otherwise perceive.

(B) "Acquisition of a new computer system" means the purchase of a "computer system," as defined in this rule, that is not a computer system currently in place nor one for which the acquisition process has been initiated as of the effective date of the board rule addressing requirements of section 1347.15 of the Revised Code.

(C) "Board" means the Ohio state board of pharmacy.

(D) "Computer system" means a "system," as defined by section 1347.01 of the Revised Code, that stores, maintains, or retrieves personal information using electronic data processing equipment.

(E) "Confidential personal information" (CPI) has the meaning as defined by division (A)(1) of section 1347.15 of the Revised Code and identified by rules promulgated by the board in accordance with division (B)(3) of section 1347.15 of the Revised Code that reference the federal or state statutes or administrative rules that make personal information maintained by the board confidential.

(F) "Employee of the board" means each employee of the board regardless of whether the employee holds an elected or appointed office or position within the board. "Employee of the board" is limited to the board of pharmacy.

(G) "Incidental contact" means contact with the information that is secondary or tangential to the primary purpose of the activity that resulted in the contact.

(H) "Individual" means natural person or the natural person's authorized representative, legal counsel, legal custodian, or legal guardian.

(I) "Information owner" means the individual appointed in accordance with division (A) of section 1347.05 of the Revised Code to be directly responsible for a system.

(J) "Person" means natural person.

(K) "Personal information" has the same meaning as defined in division (E) of section 1347.01 of the Revised Code.

(L) "Personal information system" means a "system" that "maintains" "personal information" as those terms are defined in section 1347.01 of the Revised Code.

(M) "Research" means a methodical investigation into a subject.

(N) "Routine" means common place, regular, habitual, or ordinary.

(O) "Routine information that is maintained for the purpose of internal office administration, the use of which would not adversely affect a person" as that phrase is used in division (F) of section 1347.01 of the Revised Code means personal information relating to the board's employees that is maintained by the board for administrative and human resource purposes.

(P) "System" has the same meaning as defined by division (F) of section 1347.01 of the Revised Code.

(Q) "Upgrade" means a substantial redesign of an existing system for the purpose of providing a substantial amount of new application functionality, or application modifications that would involve substantial administrative or fiscal resources to implement, but would not include maintenance, minor updates and patches, or modifications that entail a limited addition of functionality due to changes in business or legal requirements.

4729-1-08 PROCEDURES FOR ACCESSING CONFIDENTIAL PERSONAL INFORMATION

For personal information systems, whether manual or computer systems, that contain confidential personal information, the board shall do the following:

(A) Criteria for accessing confidential personal information. Personal information systems of the board are managed on a "need-to-know" basis whereby the information owner determines the level of access required for an employee of the board to fulfill the employee's job duties. The determination of access to confidential personal information shall be approved by the employee's supervisor and the information owner prior to providing the employee with access to confidential personal information within a personal information system. The board shall establish procedures for determining a revision to an employee's access to confidential personal information upon a change to that employee's job duties including, but not limited to, transfer or termination. Whenever an employee's job duties no longer require access to confidential personal information in a personal information system, the employee's access to confidential personal information shall be removed.

(B) Individual's request for a list of confidential personal information. Upon the signed written request of any individual for a list of confidential personal information about the individual maintained by the board, the board shall do the following:

(1) Verify the identity of the individual by a method that provides safeguards commensurate with the risk associated with the confidential personal information;

(2) Provide to the individual the list of confidential personal information that does not relate to an investigation about the individual or is otherwise not excluded from the scope of Chapter 1347. of the Revised Code; and

(3) If all information relates to an investigation about that individual, inform the individual that the board has no confidential personal information about the individual that is responsive to the individual's request.

(C) Notice of invalid access:

(1) Upon discovery of or notification that confidential personal information of a person has been accessed by an employee for an invalid reason, the board shall notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time. However, the board shall delay notification for a period of time necessary to ensure that the notification would not delay or impede an investigation or jeopardize homeland or national security. Additionally, the board may delay the notification consistent with any measures necessary to determine the scope of the invalid access, including which individuals' confidential personal information was invalidly accessed, and to restore the reasonable integrity of the system.

"Investigation" as used in this paragraph means the investigation of the circumstances and involvement of an employee surrounding the invalid access of the confidential personal information. Once the board determines that notification would not delay or impede an investigation, the board shall disclose the access to confidential personal information made for an invalid reason to the person.

(2) Notification provided by the board shall inform the person of the type of confidential personal information accessed and the date(s) of the invalid access.

(3) Notification may be made by any method reasonably designed to accurately inform the person of the invalid access, including written, electronic, or telephone notice.

(D) Appointment of a data privacy point of contact. The board executive director shall designate an employee of the board to serve as the data privacy point of contact. The data privacy point of contact shall work with the chief privacy officer within the office of information technology to assist the board with both the implementation of privacy protections for the confidential personal information that the board maintains and

compliances with section 1347.15 of the Revised Code and the rules adopted pursuant to the authority provided by that chapter.

(E) Completion of a privacy impact assessment. The board executive director shall designate an employee of the board to serve as the data privacy point of contact who shall timely complete the privacy impact assessment form developed by the office of information technology.

4729-1-09 VALID REASONS FOR ACCESSING CONFIDENTIAL PERSONAL INFORMATION

Pursuant to the requirements of division (B)(2) of section 1347.15 of the Revised Code, this rule contains a list of valid reasons, directly related to the board's exercise of its powers or duties, for which only authorized employees of the board or board members may access confidential personal information (CPI) regardless of whether the personal information system is a manual system or a computer system.

(A) Performing the following functions constitute valid reasons for authorized employees or members of the board to access confidential personal information:

(1) Responding to a public records request;

(2) Responding to a request from an individual for the list of CPI the board maintains on that individual;

(3) Administering a constitutional provision or duty;

(4) Administering a statutory provision or duty;

(5) Administering an administrative provision or duty;

(6) Complying with any state or federal program requirements;

(7) Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;

(8) Auditing purposes;

(9) Licensure processes;

(10) Investigation or law enforcement purposes;

(11) Administrative hearings;

(12) Litigation, complying with an order of the court, or subpoena;

(13) Human resource matters, including hiring, promotion, demotion, discharge, salary or compensation issues, processing leave requests or issues, time card approvals or issues, and payroll processing;

(14) Complying with an executive order or policy;

(15) Complying with a board policy or a state administrative policy issued by the department of administrative services, the office of budget and management or other similar state agency; or

(16) Complying with a collective bargaining agreement provision.

(B) To the extent that the general processes described in paragraph (A) of this rule do not cover the following circumstances, for the purpose of carrying out specific duties of the board, authorized employees and board members would also have valid reasons for accessing CPI in these following circumstances:

(1) Conducting a review of individuals who may be potential witnesses or other sources of information in a criminal or administrative proceeding;

(2) Administering the dangerous drug database also known as the "Ohio Automated Rx Reporting System" or "OARRS";

(3) Inspection purposes;

(4) Administering board orders; or

(5) Research performed for official duties.

4729-1-10 CONFIDENTIALITY STATUTES, REGULATIONS, AND RULES

The following federal statutes or regulations or state statutes or administrative rules make personal information maintained by the board confidential and identify the confidential personal information within the scope of rules promulgated by this board in accordance with section 1347.15 of the Revised Code:

(A) Social security numbers: 5 U.S.C. 552a, unless the individual was told that the number would be disclosed.

(B) "Bureau of Criminal Identification and Investigation" criminal records check results: section 4776.04 of the Revised Code.

(C) Student education records: 20 U.S.C. 1232g.

(D) Dangerous drug database information: division (C) of 4729.79.

(E) Personal health information: 45 C.F.R. 164.502 from the federal "Health Insurance Portability and Accountability Act of 1996 (HIPAA)."

(F) Substance abuse treatment records: section 3793.13 of the Revised Code and 42 U.S.C. 290dd-2.

(G) Records of dangerous drugs and controlled substances: section 3719.13 of the Revised Code.

(H) Security or infrastructure records: division (B) of section 149.433 of the Revised Code.

(I) Information or records that are attorney client privileged: division (A)(1) of section 2317.02 of the Revised Code.

(J) Mediation communications or records: section 2710.03 of the Revised Code.

(K) Trial preparation records: division (A)(1)(g) of section 149.43 of the Revised Code.

(L) Court filings: Rule 45(D)(1) of the rules of superintendence for the courts of Ohio.

4729-1-11 RESTRICTING AND LOGGING ACCESS TO CONFIDENTIAL PERSONAL INFORMATION IN COMPUTERIZED PERSONAL INFORMATION SYSTEMS

For personal information systems that are computer systems and contain confidential personal information, the board shall do the following:

(A) Access restrictions. Access to confidential personal information that is kept electronically shall require a password or other authentication measure.

(B) Acquisition of a new computer system. When the board acquires a new computer system that stores, manages or contains confidential personal information, the board shall include a mechanism for recording specific access by employees of the board to confidential personal information in the system.

(C) Upgrading existing computer systems. When the board modifies an existing computer system that stores, manages or contains confidential personal information, the board shall make a determination whether the modification constitutes an upgrade. Any upgrades to a computer system shall include a mechanism for

recording specific access by employees of the board to confidential personal information in the system.

(D) Logging requirements regarding confidential personal information in existing computer systems.

(1) The board shall require employees of the board who access confidential personal information within computer systems to maintain a log that records that access.

(2) Access to confidential information is not required to be entered into the log under the following circumstances:

(a) The employee of the board is accessing confidential personal information for official board purposes, including research, and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(b) The employee of the board is accessing confidential personal information for routine office procedures and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(c) The employee of the board comes into incidental contact with confidential personal information and the access of the information is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(d) The employee of the board accesses confidential personal information about an individual based upon a request made under either of the following circumstances:

(i) The individual requests confidential personal information about himself or herself.

(ii) The individual makes a request that the board take some action on that individual's behalf and accessing the confidential personal information is required in order to consider or process the request.

(3) For purposes of this paragraph, the board may choose the form or forms of logging, whether in electronic or paper formats.

(E) Log management. The board shall issue a policy that specifies the following:

(1) Who shall maintain the log:

(2) What information shall be captured in the log;

(3) How the log is to be stored; and

(4) How long information kept in this log is to be retained.

Nothing in this rule limits the board from requiring logging in any circumstance that it deems necessary.

7.0 Access Incident Report

THE OHIO STATE BOARD OF PHARMACY

Access Incident Report

On _____, the following employee accessed confidential personal information maintained by the Ohio State Board of Pharmacy. Such access is being reported pursuant to the requirements of Ohio Administrative Code 4729-1-09.

_____
Employee

_____ Valid Access

_____ Invalid Access

_____
Executive Staff Supervisor

Named Individual: _____ Case No: _____

Description of information accessed: _____
_____
_____

Description of purpose for accessing information: _____
_____
_____
_____
_____

Description of action taken: _____
_____
_____
_____
_____
_____
_____